Máximo común divisor

Elementos de Álgebra
Segundo Cuatrimestre 2022

Mg. María del Carmen Vannicola

Facultad de Informática
Departamento de Matemática

Máximo común divisor

Sea $a \in \mathbb{Z}$ y sea $D(a) = \{c \in \mathbb{Z} : c|a\}$

Se deja como ejercicio demostrar que $D(a) = D(-a)$, para todo $a \in \mathbb{Z}$ y si $a \neq 0$ entonces $D(a)$ es un conjunto finito.

Sean $a, b \in \mathbb{Z}$ y supongamos que al menos uno de ellos es distinto de cero. Definimos $D(a, b)$ como el conjunto de todos los divisores comunes de a y b, es decir,

$$D(a, b) = \{c \in \mathbb{Z} : \ c|a \ \wedge \ c|b\}.$$

Proposición

Sean $a, b \in \mathbb{Z}$, no simultáneamente nulos

1. $D(a, b) \neq \emptyset$
2. $D(a, b) = D(a) \cap D(b)$
3. $D(a, b)$ *es finito*

Demostraremos estas propiedades.

Máximo común divisor

1. $H_1)\ a, b \in \mathbb{Z} \qquad H_2)\ a \neq 0 \vee b \neq 0 \qquad T)\ D(a,b) \neq \emptyset$

   Demostración: por propiedad de la relación divide $\forall\, a \in \mathbb{Z}:\ 1|a$.

   $$1|a \wedge 1|b \overset{(1)}{\Longrightarrow} 1 \in D(a,b) \Longrightarrow D(a,b) \neq \emptyset$$

   Referencia: (1) Definición del conjunto $D(a,b)$

2. $H_1)\ a, b \in \mathbb{Z} \qquad H_2)\ a \neq 0 \vee b \neq 0 \qquad T)\ D(a,b) = D(a) \cap D(b)$

   Demostración:

   $$x \in D(a,b) \overset{(1)}{\Longleftrightarrow} x|a \wedge x|b \overset{(2)}{\Longleftrightarrow} x \in D(a) \wedge x \in D(b) \overset{(3)}{\Longleftrightarrow} x \in D(a) \cap D(b)$$

   Luego, por la definición de igualdad de conjuntos podemos concluir que

   $$D(a,b) = D(a) \cap D(b).$$

   Referencia: (1) Definición del conjunto $D(a,b)$.

   (2) Definición de los conjunto $D(a)$ y $D(b)$.

   (3) Definición de intersección de conjuntos.

3. $H_1)\ a, b \in \mathbb{Z}$ $\quad H_2)\ a \neq 0 \vee b \neq 0$ $\quad T)\ D(a, b)$ es finito

Demostración:

Por $H_2)\ a \neq 0 \vee b \neq 0$. Supongamos que $a \neq 0$.

Sea $d \in \mathbb{Z}$ tal que $d|a$ entonces $1 \leq |d| \leq |a|$ entonces existen un número finito de enteros d tales que $1 \leq |d| \leq |a|$.

Es decir existe un número finito de enteros d tales que $d|a$.

Por la proposición anterior $D(a, b) = D(a) \cap D(b)$ entonces $D(a, b) \subseteq D(a)$ y como $D(a)$ es un conjunto finito, entonces $D(a, b)$ también es un conjunto finito.

Máximo común divisor

Definición

Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos. El mayor de todos los elementos de $D(a, b)$ se llama el máximo común divisor entre a y b, y se nota (a, b).

Observemos que la definición de máximo común divisor nos asegura que

$$(a,b) = d \iff \begin{cases} d|a \ \wedge \ d|b \\ \exists\, t \in \mathbb{Z} \,/\, t|a \ \wedge \ t|b \Longrightarrow t \leq d \end{cases}$$

$$(a,b) \neq d \iff d \nmid a \ \vee \ d \nmid b \ \vee \ (\nexists\, t \in \mathbb{Z} \,/\, t|a \ \wedge \ t|b \ \wedge \ t \nleq d)$$

Máximo común divisor

Proposición

Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos.

1. $(a, b) > 0$
2. $(a, b) = (b, a)$
3. $(a, b) = (-a, b) = (a, -b) = (-a, -b) = (|a|, |b|)$
4. *Si* $b|a$ *entonces* $(a, b) = |b|$
5. $\#D(a, b) = 2 \iff (a, b) = 1$

1. $H_1)\ a, b \in \mathbb{Z} \qquad H_2)\ a \neq 0 \vee b \neq 0 \qquad T)\ (a, b) > 0$

   Demostración: (método indirecto) sea $d \in \mathbb{Z},\ d = (a, b)$ y $d \leq 0$.

   $d = (a, b) \overset{(1)}{\Longrightarrow} d|a \wedge d|b \overset{(2)}{\Longleftrightarrow} -d|a \wedge -d|b$ (3).

   $d < 0 \iff -d > 0$ (4).

   De (3) y (4) se tiene $\exists -d \in \mathbb{Z} / -d|a \wedge -d|b \wedge -d > d$ y esto contradice la definición de máximo común divisor.

Si $d = 0$ entonces 0 divide a un número distinto de cero (a o b) y esto es un absurdo.
Luego, $d > 0$ entonces $(a, b) > 0$.

Referencias. (1) Definición de máximo común divisor.

(2) Propiedad: $\forall\, x, y \in \mathbb{Z} :\ x|y \Longrightarrow -x|y$.

2. $H_1)\ a, b \in \mathbb{Z}$ $\quad H_2)\ a \neq 0 \vee b \neq 0$ $\quad T)\ (a, b) = (b, a)$

   Demostración:

$$D(a, b) = \{d \in \mathbb{Z} :\ d|a \ \wedge\ d|b\} = \{d \in \mathbb{Z} :\ d|b \ \wedge\ d|a\} = D(b, a).$$

   Como $D(a, b) = D(b, a)$ entonces el mayor elemento del conjunto $D(a, b)$ coincide con el mayor elemento del conjunto $D(b, a)$, es decir,

$$(a, b) = (b, a)$$

3. $H_1)\ a, b \in \mathbb{Z} \qquad H_2)\ a \neq 0 \vee b \neq 0 \qquad T)\ (a, b) = (-a, b)$

Demostración:

$$d \in D(a,b) \overset{(1)}{\iff} d|a \wedge d|b \overset{(2)}{\iff} d|-a \wedge d|b \overset{(1)}{\iff} d \in D(-a,b)$$

Entonces $D(a,b) = D(-a,b)$, luego el mayor entero perteneciente al conjunto $D(a,b)$ coincide con el mayor entero del conjunto $D(-a,b)$, es decir,

$$(a,b) = (-a,b).$$

Referencias: (1) Definición del conjunto $D(a,b)$.

(2) Propiedad de la relación divide. $\forall\, x, y \in \mathbb{Z} :\ x|y \Longrightarrow -x|y$.

El resto de las demostraciones de la proposición se dejan como ejercicios.

Ejemplo

Hallar el máximo común divisor entre 48 *y* -60

Utilizando la proposición anterior podemos asegurar que $(48, -60) = (48, 60)$.

Busquemos entonces los divisores comunes a 48 y 60.

Como $48 = 2 \cdot 24 = 2 \cdot 2 \cdot 12 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$ entonces

$D(48) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 8,\ \pm 12,\ \pm 16,\ \pm 24,\ \pm 48\}$

$60 = 2 \cdot 30 = 2 \cdot 2 \cdot 3 \cdot 5$ entonces

$D(60) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 5,\ \pm 6,\ \pm 10,\ \pm 12,\ \pm 15,\ \pm 20,\ \pm 30,\ \pm 60\}$

$$D(48, 60) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12\}$$

El mayor de todos los divisores comunes es 12, luego $(48, -60) = 12$

Algoritmo

Abu Abdallah Muhammad ibn Mūsā al-Jwārizmī (Abu Yāffar) conocido generalmente como **Al-Jwārizmī**, fue un matemático, astrónomo y geógrafo; persa musulmán, que vivió aproximadamente entre 780 y 850. Algunos historiadores sostienen que nació en Bagdad, otros, aseguran que nació en la ciudad Corasmia de Jiva, en el actual Uzbekistán. Estudió y trabajó en Bagdad en la primera mitad del siglo IX, en la corte del califa al-Mamun. Para muchos, fue el más grande de los matemáticos de su época. Debemos a su nombre y al de su obra principal, "Hisāb al-ŷabr wa'l muqābala", nuestras palabras álgebra, guarismo y algoritmo. De hecho, es considerado como el padre del álgebra y como el introductor de nuestro sistema de numeración denominado arábigo. Hacia 815 al-Mamun, séptimo califa Abásida, hijo de Harún al-Rashid, fundó en su capital, Bagdad, la Casa de la Sabiduría (Bayt al-Hikma), una institución de investigación y traducción que algunos han comparado con la Biblioteca de Alejandría. En ella se tradujeron al árabe obras científicas y filosóficas griegas e hindúes. En este ambiente científico se educó y trabajó Al-Jwārismī junto con otros científicos como los hermanos Banu Musa, Al-Kindi y el famoso traductor Hunayn Ibn Ishaq.

Algoritmo de Euclides

Un Algoritmo es una secuencia finita de instrucciones ordenadas y bien definidas. Por lo general utilizan un conjunto de datos de entrada y proporcionan unos datos de salida. Un algoritmo es una herramienta para resolver un problema computacional.

Proposición

Si a y b son enteros, $b \neq 0$ y r es el resto de dividir a por b entonces $D(a,b) = D(b,r)$.

Demostración: Sean q y r el cociente y el resto de dividir a por b, es decir,

$$a = bq + r,\ 0 \leq r < |b| \quad (1)$$

entonces $r = a - bq \quad (2)$.

Probemos que $D(a,b) \subseteq D(b,r)$.

$$c \in D(a,b) \overset{(3)}{\Longrightarrow} c|a \wedge c|b \overset{(4)}{\Longrightarrow} c|a \wedge c|1\cdot a+(-q)b \overset{(2)}{\Longrightarrow} c|a \wedge c|r \overset{(5)}{\Longrightarrow} c \in D(b,r).$$

Demostremos que $D(b,r) \subseteq D(a,b)$

$$c \in D(b,r) \overset{(5)}{\Longrightarrow} c|b \wedge c|r \overset{(6)}{\Longrightarrow} c|b \wedge c|qb+1\cdot r \overset{(1)}{\Longrightarrow} c|b \wedge c|a \overset{(3)}{\Longrightarrow} c \in D(a,b).$$

Algoritmo de Euclides

Referencias:

(3) Definición del conjunto $D(a, b)$ (5) Definición del conjunto $D(b, r)$

(4) Propiedad de la relación divide $c|a \wedge c|b \Longrightarrow c|xb + yc, \ \forall \ x, y \in \mathbb{Z}$.
En este caso $x = 1$ e $y = -q$

(6) Propiedad de la relación divide $c|b \wedge c|r \Longrightarrow c|xb + yr, \ \forall \ x, y \in \mathbb{Z}$.
En este caso $x = q$ e $y = 1$

Corolario

Sean $a, b \in \mathbb{Z}, \ b \neq 0$. Si r es el resto de dividir a por b entonces $(a, b) = (b, r)$.

Observemos que si $b|a$ entonces el resto de dividir a por b es cero, luego

$$(a, b) = (b, 0) = |b|$$

Algoritmo de Euclides

Ejemplo

Hallar $(48, -60)$.

Sabemos que $(48, -60) = (48, 60) = (60, 48)$

Si dividimos 60 por 48 obtenemos como cociente a 1 y resto 12, es decir,

$$60 = 48 \cdot 1 + 12.$$

El corolario anterior nos asegura que

$$(60, 48) = (48, 12)$$

Utilizando la observación que está despúes del corolario y como $12|48$ tenemos que $(48, 12) = 12$. Luego

$$(60, 48) = 12.$$

Algoritmo de Euclides

Ejemplo

Hallar $(495, 144)$

Busquemos el resto de dividir 495 por 144.

Como $495 = 144 \cdot 3 + 63$ entonces $(495, 144) = (144, 63)$ (1)

Ahora repitamos este proceso. $144 = 63 \cdot 2 + 18$ entonces $(144, 63) = (63, 18)$ (2)

Al dividir 63 por 18 obtenemos resto 9, luego $(63, 18) = (18, 9)$ (3)

y al dividir 18 por 9 obtenemos resto cero, luego $(18, 9) = (9, 0) = 9$ (4)

Entonces

$$(495, 144) \overset{(1)}{=} (144, 63) \overset{(2)}{=} (63, 18) \overset{(3)}{=} (18, 9) \overset{(4)}{=} (9, 0) = 9$$

Algoritmo de Euclides

Sean a y b dos enteros no simultáneamente nulos. Como $(a, b) = (a, -b)$ podemos suponer sin pérdida de generalidad, que a y b son enteros positivos. Consideremos las siguientes divisiones sucesivas:

$$\begin{array}{rcll}
a & = & b \cdot q_1 + r_1, & \text{con } 0 < r_1 < b \\
b & = & r_1 \cdot q_2 + r_2, & \text{con } 0 < r_2 < r_1 \\
r_1 & = & r_2 \cdot q_3 + r_3, & \text{con } 0 < r_3 < r_2 \\
 & \vdots & & \\
r_i & = & r_{i+1} \cdot q_{i+2} + r_{i+2}, & \text{con } 0 < r_{i+2} < r_{i+1}, \text{ donde } 2 \leq i \leq n-3 \\
 & \vdots & & \\
r_{n-2} & = & r_{n-1} \cdot q_n + r_n, & \text{con } 0 < r_n < r_{n-1} \\
r_{n-1} & = & r_n \cdot q_{n+1}. &
\end{array}$$

Como al cabo de un número finito de pasos obtenemos un resto nulo, aplicando el corolario anterior podemos asegurar que

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n.$$

Algoritmo de Euclides

El algoritmo se puede esquematizar de la siguiente manera:

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4	$\cdots$	r_n	0	

Luego $(a, b) = r_n$, pues r_n es el último resto no nulo. Si el resto es cero en la primera división entonces a es múltiplo de b y $(a, b) = b$.

Retomaremos los ejemplos anteriores y haremos el esquema del Algoritmo de Euclides.

Ejemplo

Hallar $(48, -60)$.

Sabemos que $(48, -60) = (48, 60) = (60, 48)$

Si dividimos 60 por 48 obtenemos como cociente a 1 y resto 12, es decir $60 = 48 \cdot 1 + 12$.

El corolario nos asegura que

$$(60, 48) = (48, 12)$$

Algoritmo de Euclides

Realizando el esquema del Algoritmo de Euclides tenemos

	1	4
60	48	12
12	0	

Observamos en el esquema que el último resto no nulo es 12. Luego

$$(48, -60) = 12.$$

Ejemplo

Hallar $(495, 144)$.

Por lo desarrollado en la página 14 tenemos

$495 = 144 \cdot 3 + 63 \Longrightarrow (495, 144) = (144, 63)$

$144 = 63 \cdot 2 + 18 \Longrightarrow (144, 63) = (63, 18)$

Algoritmo de Euclides

$63 = 18 \cdot 3 + 9 \Longrightarrow (63, 18) = (18, 9)$

$18 = 9 \cdot 2 + 0 \Longrightarrow (18, 9) = (9, 0) = 9$

Entonces

	3	2	3	2
495	144	63	18	9
63	18	9	0	

De lo que decucimos

$$(495, 144) = 9$$

Ya que el máximo común divisor entre 495 y 144 es el último resto no nulo en el esquema del Algoritmo.

Algoritmo de Euclides

Teorema

Dados $a, b \in \mathbb{Z},\ b \neq 0$, existen enteros x e y tales que $(a, b) = xa + yb$.

Observación: Los valores $x, y \in \mathbb{Z}$ tales que $(a, b) = xa + yb$ no son únicos, por ejemplo si consideramos $a = 2$ y $b = 5$ entonces $(2, 5) = 1$ y

$\exists\, x, y \in \mathbb{Z},\ x = -2,\ y = 1 / \ 1 = (-2)2 + 1 \cdot 5$

$\exists\, x, y \in \mathbb{Z},\ x = -7,\ y = 3 / \ 1 = (-7)2 + 3 \cdot 5$

$\exists\, x, y \in \mathbb{Z},\ x = 8,\ y = -3 / \ 1 = 8 \cdot 2 + (-3)5$

Ejemplo

Encontrar valores $x, y \in \mathbb{Z}$ tales que

$$(495, 144) = 495x + 144y$$

Algoritmo de Euclides

Según las divisiones realizadas en el algoritmo tenemos

$495 = 3 \cdot 144 + 63$ entonces $63 = 495 + (-3)144 \quad (1)$

$144 = 2 \cdot 63 + 18$ entonces $18 = 144 + (-2)63 \quad (2)$

$63 = 3 \cdot 18 + 9$ entonces $9 = 63 + (-3)18$

$$9 = 63 + (-3)18 \overset{(2)}{=} 63 + (-3)(144 + (-2)63) = 63 + (-3)144 + 6 \cdot 63 =$$

$$= 7 \cdot 63 + (-3)144 \overset{(1)}{=} 7(495 + (-3)144) + (-3)144 = 7 \cdot 495 + (-21)144 + (-3)144 =$$

$$= 7 \cdot 495 + (-24)144$$

Luego $\exists\, x, y \in \mathbb{Z},\ x = 7,\ y = -24 /\ 9 = 495x + 144y$

Como $(495, 144) = 9$ entonces $\exists x, y \in \mathbb{Z},\ x = 7,\ y = -24 /\ (495, 144) = 495x + 144y$

Algoritmo de Euclides

Observemos que si existen $x, y \in \mathbb{Z}$ tales que $(a, b) = xa + yb$ entonces

$\exists\, x_1, y_1 \in \mathbb{Z},\ x_1 = -x,\ y_1 = y /\ (-a, b) = x_1(-a) + y_1 b$

$\exists\, x_2, y_2 \in \mathbb{Z},\ x_2 = x,\ y_2 = -y /\ (a, -b) = x_2 a + y_2(-b)$

$\exists\, x_3, y_3 \in \mathbb{Z},\ x_3 = -x,\ y_3 = -y /\ (-a, -b) = x_3(-a) + y_3(-b)$

En nuestro ejemplo:

$(-495, 144) = (495, 144) = 9$ y $9 = 7 \cdot 495 + (-24)144 = (-7)(-495) + (-24)144$

$$(-495, 144) = (-7)(-495) + (-24)144$$

$(495, -144) = (495, 144) = 9$ y $9 = 7 \cdot 495 + (-24)144 = 7 \cdot 495 + 24(-144)$

$$(495, -144) = 7 \cdot 495 + 24(-144)$$

$(-495, -144) = (495, 144) = 9$ y $9 = 7 \cdot 495 + (-24)144 = (-7)(-495) + 24(-144)$

$$(-495, -144) = (-7)(-495) + 24(-144)$$

Algoritmo de Euclides

Reformulemos el ejemplo anterior

Ejemplo

Analizar si existe $x \in \mathbb{Z}$ *tal que* $144|495x - 18$

Si $144|495x - 18$ entonces existe $y \in \mathbb{Z}$ tal que $495x - 18 = 144y$, luego

$$495x - 144y = 18$$

Considerando el ejemplo anterior, existen $x = 7$ e $y = 24$ tales que

$$9 = 7 \cdot 495 + 24(-144)$$

$18 = 2 \cdot 9 = 2(7 \cdot 495 + 24(-144)) = 14 \cdot 495 + 48(-144)$, luego

$$\exists\ x, y \in \mathbb{Z},\ x = 14,\ y = 48/\ 18 = 14 \cdot 495 + 48(-144)$$

De lo que deducimos

$$\exists\ x \in \mathbb{Z},\ x = 14/\ 144|495x - 18$$

Algoritmo de Euclides

Las siguientes proposiciones son una consecuencia de expresar el máximo común divisor entre a y b como una combinación lineal entera de los enteros a y b.

Proposición

Sean $a, b, c \in \mathbb{Z}$, a y b no simultáneamente nulos. Entonces existen enteros x e y tales que

$$ax + by = c \text{ si y sólo si } (a, b)|c.$$

Proposición

Sean $a, b \in \mathbb{Z}$, a y b no simultáneamente nulos. Entonces existen enteros x e y tales que

$$ax + by = 1 \text{ si y sólo si } (a, b) = 1.$$

Ejemplo

Analizar los posibles valores que puede tomar (a, b)*, sabiendo que* $3a + 12b = 6$ *y* b *es impar.*

Sabemos que si existen $x, y \in \mathbb{Z}$ tales que $ax + by = c$ entonces $(a, b)|c$. Luego

$$(a, b)|6$$

De lo que deducimos $(a, b) \in \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 6\}$

Como $(a, b) > 0$ entonces $(a, b) \in \{1,\ 2,\ 3,\ 6\}$

- $(a, b) = 2 \overset{(1)}{\Longrightarrow} 2|a \ \wedge\ 2|b \overset{(2)}{\Longrightarrow} 2|b$, luego b es par y esto contradice uno de los datos del ejercicio. Deducimos entonces que

$$(a, b) \neq 2$$

- $(a, b) = 6 \overset{(1)}{\Longrightarrow} 6|a \ \wedge\ 6|b \overset{(2)}{\Longrightarrow} 6|b \quad (3)$

Algoritmo de Euclides

Por otra parte

$2|6 \overset{(3)}{\Longrightarrow} 2|6 \wedge 6|b \overset{(4)}{\Longrightarrow} 2|b$, es decir, b es par. Nuevamente hemos contradecido la hipótesis, entonces

$$(a, b) \neq 6$$

Luego $(a, b) = 1$ o $(a, b) = 3$.

Referencias: (1) Definición de máximo común divisor.
(2) Simplificación.
(4) Transitividad de la relación divide.

Ejemplo

Si $7a + 5b = 18$, $(a, b) \neq 1$ *y* $(3, b) = 1$, *hallar* (a, b).

Como si existen $x, y \in \mathbb{Z}$ tales que $ax + by = c$ entonces $(a, b)|c$,

$$(a, b)|18$$

Luego $(a, b) \in \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 6,\ \pm 9,\ \pm 18\}$

Algoritmo de Euclides

Considerando que $(a, b) > 0$ tenemos $(a, b) \in \{1,\ 2,\ 3,\ 6,\ 9,\ 18\}$

- $(a, b) = 3 \overset{(1)}{\Longrightarrow} 3|a \ \wedge\ 3|b \overset{(2)}{\Longrightarrow} 3|b \overset{(3)}{\Longrightarrow} (3, b) = 3$

  $(3, b) = 3$ contradice que $(3, b) = 1$. Por esto:

  $$(a, b) \neq 3$$

- $(a, b) = 18 \overset{(1)}{\Longrightarrow} 18|a \ \wedge\ 18|b \overset{(2)}{\Longrightarrow} 18|b\ \ (4).$

  Además $3|18 \overset{(4)}{\Longrightarrow} 3|18 \ \wedge\ 18|b \overset{(5)}{\Longrightarrow} 3|b \overset{(3)}{\Longrightarrow} (3, b) = 3$

  Esto contradice el hecho que $(3, b) = 1$, luego $(a, b) \neq 18$.

- Análogamente se prueba que $(a, b) \neq 9$ y $(a, b) \neq 6$.

Como $(a, b) \neq 1$ entonces $(a, b) = 2$

Referencias: (1) Definición de máximo común divisor. (2) Simplificación.
(3) Propiedad: $x|y \Longrightarrow (x, y) = |x|$. (5) Transitividad de la relación divide.

Propiedades

Proposición

Sean $a, b, c \in \mathbb{Z}$.

1. $(a,(b,c)) = ((a,b),c)$, a, b *y* c *no simultáneamente nulos.*
2. $(ac, bc) = |c|(a,b)$, $c \neq 0$
3. $(a + cb, b) = (a,b)$

Ejemplo

Sabiendo que $(a, 23) = 6$, *calcular* $(2a + 46, -46)$

Por hipótesis,

$$(a,23) = 6 \overset{Prop\,2}{\Longrightarrow} (-2a,(-2)23) = |-2|6 \implies (-2a,-46) = 12 \implies$$

$$\implies (2a,-46) = 12 \overset{Prop\,3}{\Longrightarrow} (2a + (-1)(-46),-46) = (2a,-46) = 12 \implies$$

$$\implies (2a + 46,-46) = 12$$

Ejemplo

Ejemplo

Demostrar que $(21 + 18b,\ 6b) = 3,$ *si* $(7,\ b) = 1$

$$(21 + 18b,\ 6b) = (3(7 + 6b),\ 3(2b)) \overset{Prop\,2}{=} |3|(7 + 6b,\ 2b) =$$

$$= 3(7 + 3(2b),\ 2b) \overset{Prop\,3}{=} 3(7,\ 2b) \quad (1)$$

Por (1) debemos probar que $3(7, 2b) = 3$ lo que equivale a demostrar que $(7, 2b) = 1$

Por hipótesis $(7, b) = 1$ entonces 1 es el mayor número del conjunto $D(7, b)$

$$D(7, b) = D(7) \cap D(b) = \{-7, -1, 1, 7\} \cap D(b) = \{-1,\ 1\}$$

Entonces $7 \notin D(b)$ y $-7 \notin D(b)$, es decir, $7 \nmid b$ y $-7 \nmid b$. Por el teorema de la división entera

$$\exists\, q, r \in \mathbb{Z} /\ b = 7q + r,\ 0 < r < 7$$

Luego $\exists\, q, r \in \mathbb{Z} /\ 2b = 7(2q) + 2r, \quad r = 1,\ 2,\ 3,\ 4,\ 5,\ 6$

Ejemplo

$b = 7q + r$	$2b = 7(2q) + 2r$	$2b = 7t + s,\ 0 < s < 7$
$b = 7q + 1$	$2b = 7(2q) + 2$	$2b = 7t + 2,\ 0 < 2 < 7$
$b = 7q + 2$	$2b = 7(2q) + 4$	$2b = 7t + 4,\ 0 < 4 < 7$
$b = 7q + 3$	$2b = 7(2q) + 6$	$2b = 7t + 6,\ 0 < 6 < 7$
$b = 7q + 4$	$2b = 7(2q) + 8 = 7(2q) + 7 + 1$	$2b = 7(t + 1) + 1,\ 0 < 1 < 7$
$b = 7q + 5$	$2b = 7(2q) + 10 = 7(2q) + 7 + 3$	$2b = 7(t + 1) + 3,\ 0 < 3 < 7$
$b = 7q + 6$	$2b = 7(2q) + 12 = 7(2q) + 7 + 5$	$2b = 7(t + 1) + 5,\ 0 < 5 < 7$

Ejemplo

En la tabla que el resto de dividir a $2b$ por 7 es distinto de cero, cuando $7 \nmid b$ entonces

$$7 \nmid 2b \iff 7 \notin D(2b)$$

Luego

$$D(7, 2b) = D(7) \cap D(2b) = \{-7, -1, 1, 7\} \cap D(2b) = \{-1, 1\}$$

Como 1 es el mayor número del conjunto $\{-1, 1\}$ entonces $(7, 2b) = 1$, de lo que deducimos $3(7, 2b) = 3$

Retomando (1), tenemos

$$(21 + 18b, 6b) = 3(7, 2b) = 3$$

Coprimos

Definición

Sean $a, b \in \mathbb{Z}$ se dice que a y b son **coprimos** *o* **relativamente primos** *si y sólo si* $(a, b) = 1$

Observaciones:

1. Si $(a, b) = 1$ entonces los únicos divisores comunes son 1 y -1.
2. $(a, b) = 1$ es equivalente a la existencia de $x, y \in \mathbb{Z}$ tales que $ax + by = 1$

$(12, 35) = 1$, pero 12 y 15 no son coprimos, pues $(12, 15) = 3$

Teorema

Sean $a, b, c \in \mathbb{Z}$. Si $a|bc$ y a y b son relativamente primos entonces $a|c$

$H_1) a|bc \qquad H_2)\ (a, b) = 1 \qquad T)\ a|c$

Demostración:

$$(a, b) = 1 \implies \exists\, x, y \in \mathbb{Z} /\ 1 = xa + yb \implies \exists\, x, y \in \mathbb{Z} /\ c = xac + ybc \quad (1)$$

Coprimos

Por propiedad de divisibilidad (página 9-item 5) $\forall\, a \in \mathbb{Z}:\ a|a \Longrightarrow a|ac$, , entonces

$$a|ac \overset{H_1)}{\Longrightarrow} a|ac \wedge a|bc \overset{(2)}{\Longrightarrow} a|xac + ybc \overset{(1)}{\Longrightarrow} a|c$$

Referencia: (2) Propiedad de divisibilidad: $a|b \wedge a|c \Longrightarrow a|xb + yc,\ \forall\, x, y \in \mathbb{Z}$

Teorema

Sean $a, b, c \in \mathbb{Z}$. Si $a|c$, $b|c$ y a y b son coprimos entonces $ab|c$

$H_1)\ a|c \qquad H_2)\ b|c \qquad H_3)\ (a, b) = 1 \qquad T)\ ab|c$

Demostración:

Por $H_3)$, $(a, b) = 1 \Longrightarrow \exists\, x, y \in \mathbb{Z}\ /\ 1 = xa + yb \Longrightarrow$

$$\exists\, x, y \in \mathbb{Z}\ /\ c = xac + ybc \quad (1)$$

Por $H_1)$, $H_2)$ $a|c \wedge b|c \Longrightarrow \exists\, t, s \in \mathbb{Z}\ /\ c = at \wedge c = bs \overset{(1)}{\Longrightarrow}$

$$\exists\, t, s \in \mathbb{Z}\ /\ c = xabs + ybat = xsab + ytab = (xs + yt)ab.$$

Coprimos

Proposición

Sean $a, b, c \in \mathbb{Z}$.

1. *Si* $(a, b) = 1$ *entonces* $(a \pm b, b) = 1$
2. *Si* $(a, b) = 1$ *entonces* $(a + b, ab) = 1$
3. *Si* $(a, c) = 1$ *y* $(b, c) = 1$ *entonces* $(ab, c) = 1$
4. *Si* $(a, b) = 1$ *entonces* $(a^n, b^m) = 1$, *para todo* $n, m \in \mathbb{N}_0$

Proposición

Sean $a, b, c \in \mathbb{Z}$.

1. *Si* $(a, b) = d$ *entonces* $(\frac{a}{d}, \frac{b}{d}) = 1$
2. *Si* $(a, b) = 1$ *entonces* $(ac, b) = (c, b)$, *cualquiera sea* $c \in \mathbb{Z}$

Números primos

Si $a \in \mathbb{Z}, a \neq 0$, entonces a posee al menos los siguientes divisores:

$$1, \ -1, \ a, \ -a$$

Estos divisores se llaman **divisores triviales** de a. A todo divisor distinto de los triviales, se lo llama **divisor propio** de a.

Definición

Un número entero "a" distinto de $0, \ 1$ *y* -1*, se dice* **primo** *si sus únicos divisores son los triviales.*

La definición anterior es equivalente a decir que un entero diferente de $0, \ 1$ y -1 es primo si tiene exactamente cuatro divisores, que son: $1, \ -1, \ a$ y $-a$.

Definición

A todo número entero "a" distinto de $0, \ 1$ *y* -1*, que no sea primo, se le llama* **compuesto**.

Observemos que si "a" es un número compuesto entonces existe $b \in \mathbb{Z}$, $b \neq 0, 1, -1, a, -a$ tal que $b|a$

Números primos

Todo número compuesto a puede escribirse de la forma

$$a = t \cdot r$$

donde $t, r \in \mathbb{Z}, t \neq \pm 1$ y $r \neq \pm 1$

Son ejemlos de números primos $-91, -31, 7$ y 19 y de números compuestos $-39, 15$ y 78

Observemos que el conjunto de los números enteros está particionado por tres subconjuntos disjuntos

$$\mathbb{Z} = \{0, 1, -1\} \cup \{a \in \mathbb{Z} : \ a \text{ es primo}\} \cup \{a \in \mathbb{Z} : \ a \text{ es compuesto}\}$$

Teorema

Todo número entero a distinto de $0, 1$ y -1 admite por lo menos un divisor primo positivo.

El teorema anterior nos asegura que, si $a \in \mathbb{Z}, \ a \neq 0, 1, -1$ entonces

$$\exists\, p \in \mathbb{Z} / \ \ \text{p es primo} \wedge p|a$$

Números primos

Teorema

(Euclides) Existen infinitos números primos.

Proposición

Sean $a, b \in \mathbb{Z}$.

1. *Dado un número primo* p, *si* $p \nmid a$ *entonces* $(p, a) = 1$.
2. *Sea* p *un número primo. Si* $p|ab$ *entonces* $p|a$ *o* $p|b$.

Demostración:

1. La demostración de esta propiedad se propone como ejercicio.
2. $H_1)$ p es un número primo $\qquad H_2)$ $p|ab \qquad T)$ $p|a \vee p|b$

   Supongamos que $p \nmid a$ y probemos que $p|b$

   $p \nmid a \overset{(1)}{\Longrightarrow} (p, a) = 1 \overset{(2)}{\Longrightarrow} p|b.$

   Referencias: (1) Item 1. de esta propiedad.
   (2) Por Teorema (página 31) y $H_2)$ $p|ab \wedge (p, a) = 1 \Longrightarrow p|b$

Números primos

El siguiente teorema nos proporciona un mecanismo simple para saber si un número es primo o no.

Teorema

Sea $n \in \mathbb{Z},\ n > 1$. Si n no es primo entonces existe un primo p tal que $p|n$ y $p \leq \sqrt{n}$.

Podemos ejemplificar este teorema tomando $n = 91$. Como la parte entera de $\sqrt{91}$ es 9, debemos considerar los enteros primos positivos menores o iguales a 9, es decir,

$$p \in \{2, 3, 5, 7\}$$

y controlar si $p|91$ para algún $p \in \{2, 3, 5, 7\}$.

Sabemos que 7 divide a 91, de lo que deducimos que 91 no es primo.

Si consideramos $n = 97$, como a parte entera de $\sqrt{97}$ es 9 y

$$2 \nmid 97, \quad 3 \nmid 97, \quad 5 \nmid 97, \quad 7 \nmid 97$$

entonces podemos concluír que 97 es primo.

Teorema Fundamental de la Aritmética

Teorema

(Teorema Fundamental de la Aritmética) Todo número entero a distinto de 0, 1 y -1, es un número primo o bien se puede escribir como ± 1 por un producto de números primos positivos. Esta representación de un entero como producto de primos es única, salvo el orden de los factores.

Sea $a \in \mathbb{Z}$, $a \neq 0, 1, -1$. Entonces a es primo o

$\exists\, p_1, p_2, \ldots, p_r \in \mathbb{N}$, p_i primos, $1 \leq i \leq r$ tales que

$$a = \pm\, p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

Observemos que agrupando los factores primos iguales entre sí en la representación $a = \pm\, p_1 \cdot p_2 \cdot \ldots \cdot p_r$, podemos escribir

$$a = \pm\, p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$$

donde ahora los primos $p_1, p_2, \ldots, p_s$ son distintos dos a dos, $e_i \in \mathbb{N}$, $1 \leq i \leq s$.

Números primos

El siguiente teorema nos proporciona una herramienta para hallar los divisores positivos de un número entero a dado.

Sin pérdida de generalidad, podemos considerar $a > 1$ ya que los divisores de a y de $-a$ coinciden.

Teorema

Sea $a > 1$ y sea $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$, donde los p_i son primos distintos dos a dos, y $e_i \in \mathbb{N}$, con $1 \leq i \leq s$. Sea $b \in \mathbb{Z}$, $b > 0$, entonces

$$b|a \iff b = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_s^{t_s}, \quad 0 \leq t_i \leq e_i, \quad \text{para} \quad 1 \leq i \leq s.$$

Hallados los divisores positivos de a, todos sus divisores se obtienen calculando los opuestos de los divisores positivos encontrados.

De forma inmediata al teorema anterior, podemos hallar la cantidad de divisores de un número entero dado.

Sea $a \in \mathbb{Z}$, $a > 1$, $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$, llamaremos con $d(a)$ al **número de divisores positivos de** a. Luego

$$d(a) = (e_1 + 1) \cdot (e_2 + 1) \cdot \ldots \cdot (e_n + 1).$$

Ejemplo

Indicar que cantidad de divisores que tiene 7800 y hallarlos.

7800 se factoriza en primos de la siguiente manera

$$7800 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 13 = 2^3 \cdot 3 \cdot 5^2 \cdot 13 = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot 13^{e_4}$$

Sabemos que la cantidad de divisores positivos de 7800 es

$$d(a) = (e_1+1)\cdot(e_2+1)\cdot(e_3+1)\cdot(e_4+1) = (3+1)(1+1)(2+1)(1+1) = 4\cdot 2\cdot 3\cdot 2 = 48$$

La cantidad de divisores de 7800 es

$$2d(a) = 2 \cdot 48 = 96$$

Veamos ahora cuáles son estos divisores

Sabemos que $b|7800$ si y sólo si $b = \pm 2^{t_1} \cdot 3^{t_2} \cdot 5^{t_3} \cdot 13^{t_4}$, donde

Teorema Fundamental de la Aritmética

$b = \pm 2^{t_1} \cdot 3^{t_2} \cdot 5^{t_3} \cdot 13^{t_4}$, donde

$t_1 = 0, 1, 2, 3 \quad t_2 = 0, 1 \quad t_3 = 0, 1, 2 \quad t_4 = 0, 1.$ Entonces

$b = \pm 2^0 \cdot 3^0 \cdot 5^0 \cdot 13^0 = \pm 1$
$b = \pm 2^0 \cdot 3^0 \cdot 5^1 \cdot 13^0 = \pm 5$
$b = \pm 2^0 \cdot 3^0 \cdot 5^2 \cdot 13^0 = \pm 25$

$b = \pm 2^0 \cdot 3^0 \cdot 5^0 \cdot 13^1 = \pm 13$
$b = \pm 2^0 \cdot 3^0 \cdot 5^1 \cdot 13^1 = \pm 5 \cdot 13 = \pm 65$
$b = \pm 2^0 \cdot 3^0 \cdot 5^2 \cdot 13^1 = \pm 25 \cdot 13 = \pm 325$

$b = \pm 2^0 \cdot 3^1 \cdot 5^0 \cdot 13^0$
$b = \pm 2^0 \cdot 3^1 \cdot 5^1 \cdot 13^0$
$b = \pm 2^0 \cdot 3^1 \cdot 5^2 \cdot 13^0$

$b = \pm 2^0 \cdot 3^1 \cdot 5^0 \cdot 13^1$
$b = \pm 2^0 \cdot 3^1 \cdot 5^1 \cdot 13^1$
$b = \pm 2^0 \cdot 3^1 \cdot 5^2 \cdot 13^1$

$b = \pm 2^1 \cdot 3^0 \cdot 5^0 \cdot 13^0$
$b = \pm 2^1 \cdot 3^0 \cdot 5^1 \cdot 13^0$
$b = \pm 2^1 \cdot 3^0 \cdot 5^2 \cdot 13^0$

$b = \pm 2^1 \cdot 3^0 \cdot 5^0 \cdot 13^1$
$b = \pm 2^1 \cdot 3^0 \cdot 5^1 \cdot 13^1$
$b = \pm 2^1 \cdot 3^0 \cdot 5^2 \cdot 13^1$

$b = \pm 2^1 \cdot 3^1 \cdot 5^0 \cdot 13^0$
$b = \pm 2^1 \cdot 3^1 \cdot 5^1 \cdot 13^0$
$b = \pm 2^1 \cdot 3^1 \cdot 5^2 \cdot 13^0$

$b = \pm 2^1 \cdot 3^1 \cdot 5^0 \cdot 13^1$
$b = \pm 2^1 \cdot 3^1 \cdot 5^1 \cdot 13^1$
$b = \pm 2^1 \cdot 3^1 \cdot 5^2 \cdot 13^1$

Teorema Fundamental de la Aritmética

$b = \pm 2^2 \cdot 3^0 \cdot 5^0 \cdot 13^0$ $\quad$ $b = \pm 2^2 \cdot 3^0 \cdot 5^0 \cdot 13^1$

$b = \pm 2^2 \cdot 3^0 \cdot 5^1 \cdot 13^0$ $\quad$ $b = \pm 2^2 \cdot 3^0 \cdot 5^1 \cdot 13^1$

$b = \pm 2^2 \cdot 3^0 \cdot 5^2 \cdot 13^0$ $\quad$ $b = \pm 2^2 \cdot 3^0 \cdot 5^2 \cdot 13^1$

$b = \pm 2^2 \cdot 3^1 \cdot 5^0 \cdot 13^0$ $\quad$ $b = \pm 2^2 \cdot 3^1 \cdot 5^0 \cdot 13^1$

$b = \pm 2^2 \cdot 3^1 \cdot 5^1 \cdot 13^0$ $\quad$ $b = \pm 2^2 \cdot 3^1 \cdot 5^1 \cdot 13^1$

$b = \pm 2^2 \cdot 3^1 \cdot 5^2 \cdot 13^0$ $\quad$ $b = \pm 2^2 \cdot 3^1 \cdot 5^2 \cdot 13^1$

$b = \pm 2^3 \cdot 3^0 \cdot 5^0 \cdot 13^0$ $\quad$ $b = \pm 2^3 \cdot 3^0 \cdot 5^0 \cdot 13^1$

$b = \pm 2^3 \cdot 3^0 \cdot 5^1 \cdot 13^0$ $\quad$ $b = \pm 2^3 \cdot 3^0 \cdot 5^1 \cdot 13^1$

$b = \pm 2^3 \cdot 3^0 \cdot 5^2 \cdot 13^0$ $\quad$ $b = \pm 2^3 \cdot 3^0 \cdot 5^2 \cdot 13^1$

$b = \pm 2^3 \cdot 3^1 \cdot 5^0 \cdot 13^0$ $\quad$ $b = \pm 2^3 \cdot 3^1 \cdot 5^0 \cdot 13^1$

$b = \pm 2^3 \cdot 3^1 \cdot 5^1 \cdot 13^0$ $\quad$ $b = \pm 2^3 \cdot 3^1 \cdot 5^1 \cdot 13^1$

$b = \pm 2^3 \cdot 3^1 \cdot 5^2 \cdot 13^0$ $\quad$ $b = \pm 2^3 \cdot 3^1 \cdot 5^2 \cdot 13^1$

Máximo común divisor

La siguiente proposición nos da un método para calcular el máximo común divisor entre dos números enteros a partir de sus descomposiciones en factores primos.

Proposición

Sean $a, b \in \mathbb{Z}$, $a \geq 0$, $b \geq 0$, *a y b no simultáneamente nulos.*

Si $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ *y* $b = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_s^{t_s}$; *con* $e_i \geq 0$, $t_i \geq 0$ *para* $1 \leq i \leq s$, *entonces*

$$(a, b) = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_s^{m_s},$$

donde m_i *es el menor de los números* e_i *y* t_i, *para* $1 \leq i \leq s$.

Observación: si a o b son menores que cero, entonces podemos considerar la descomposoción en primos de $|a|$ y $|b|$ para hacer los cálculos, ya que $(a, b) = (-a, b) = (a, -b) = (-a, -b)$. Es decir, podemos considerar en la descomposición de productos de potencias de primos, números primos positivos.

Máximo común divisor

Ejemplo

Hallar el máximo común divisor entre -7800 *y* 4080

Como $(-7800, 4080) = (7800, 4080)$, haremos la descomposición en factores primos de los números 7800 y 4080. Entonces

$7800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13$ $\qquad$ $4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$

$7800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13 \cdot 17^0$ $\qquad$ $4080 = 2^4 \cdot 3 \cdot 5 \cdot 13^0 \cdot 17$

$$(7800, 4080) = 2^3 \cdot 3 \cdot 5 \cdot 13^0 \cdot 17^0 = 2^3 \cdot 3 \cdot 5 = 120$$

Ejemplo

Sean $a, b \in \mathbb{Z}$. *Analizar si la siguiente proposición es verdadera o falsa y justificar.*
"Si p, q, r *son primos distintos,* $a = p^2 \cdot q$ *y* $b = p \cdot q^3 \cdot r$ *entonces* $(a, b) = p \cdot q$ *"*

El siguiente razonamiento es INCORRECTO. Buscar el error y hacer un desarrollo válido para justificar que la proposición enunciada es Falsa

$a = p^2 \cdot q = p^2 \cdot q^1 \cdot r^0$ y $b = p \cdot q^3 \cdot r = p^1 \cdot q^3 \cdot r^1$ utilizando la propiedad de la página anterior

$(a, b) = p^1 \cdot q^1 \cdot r^0 = p \cdot q$, entonces, la proposición es verdadera.

Ejercicio

Sean $a,\ b,\ c,\ d \in \mathbb{Z},\ b \neq 0$. *Indicar el valor de verdad de las siguientes proposiciones. Justificar cada uno de los razonamientos.*

1. *Si* $a = p^2q^3$ *con* $p,\ q$ *números primos distintos y* $a|b$ *entonces* $24 \leq |D(b)|$
2. $\forall\, b \in \mathbb{N} :\ (b^3,\ b^5) = b^3$
3. $\forall\, b \in \mathbb{Z} :\ (b^3,\ b^5) = b^3$
4. *Si* $5a - 13b = 6$ *y* $(a, 2) = 1$ *entonces* a *y* b *son coprimos*
5. $\forall\, a, b, c \in \mathbb{Z},\ b \neq 0 :\ (ac, bc) = |c|(a, b)$
6. $\exists\, a \in \mathbb{Z} / \forall\, b \in \mathbb{Z} - \{0\} : D(a, b) = D(a) \ \wedge\ a \nmid b$
7. *Si* $a|c,\ b|c$ *y* $2 \in D(a, b)$ *entonces* $ab|c$
8. *Sean* $p,\ q,\ r$ *primos distintos dos a dos. Si* $a = p^2q^2$ *y* $b = pq^2r^2$ *entonces* $(ra,\ -b^2) = |r|(a, pb)$